PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-027417
(43)Date of publication of application : 25.01.2002

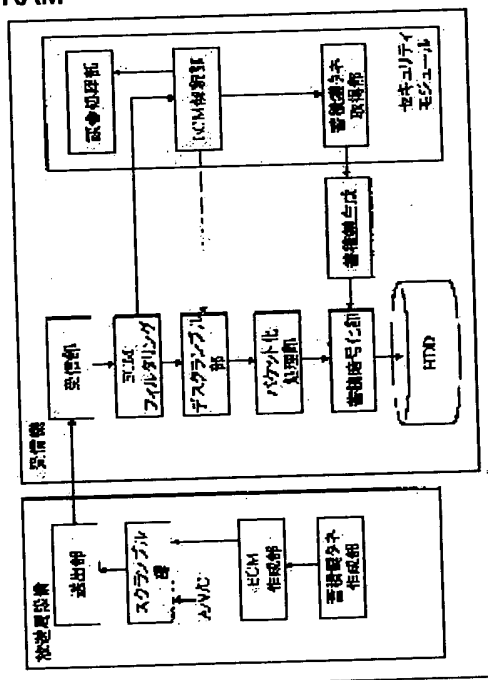
(51)Int.CI. H04N 7/08
H04N 7/081
H04H 1/00
H04L 9/08
H04N 5/44
H04N 5/765
H04N 5/781
H04N 7/16
H04N 7/167

(21)Application number : 2000-208076
(22)Date of filing : 10.07.2000

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MATSUO TAKASHI
INOUE TETSUYA
MURAKAMI HIRONORI
NIWANO SATOSHI
AZUMA AKIO
NAKAHARA TORU
FUKAMI YUKIYASU

(54) METHOD AND DEVICE FOR ACCUMULATING PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method and device for limited reception which realizes a safe conditional access, related to an accumulation broadcast method where broadcasted programs are accumulated and then reproduce for viewing at a convenient time.
SOLUTION: An accumulation coding part is provided where an accumulation encryption is processed, a plurality of accumulation encryption keys are generated and the accumulation encryption key is changed corresponding to an accumulation packet, for higher security for accumulated contents.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－27417
（P2002－27417A）
(43)公開日　平成14年１月25日(2002.1.25)

(51)Int.Cl.⁷		識別記号	FI			テーマコード（参考）
H04N	7/08		H04H	1/00	F	5C025
	7/081		H04N	5/44	A	5C063
H04H	1/00			7/16	C	5C064
H04L	9/08			7/08	Z	5J104
H04N	5/44		H04L	9/00	601D	

審査請求　未請求　請求項の数12　ＯＬ　（全５頁）　最終頁に続く

(21)出願番号　特願2000－208076(P2000－208076)

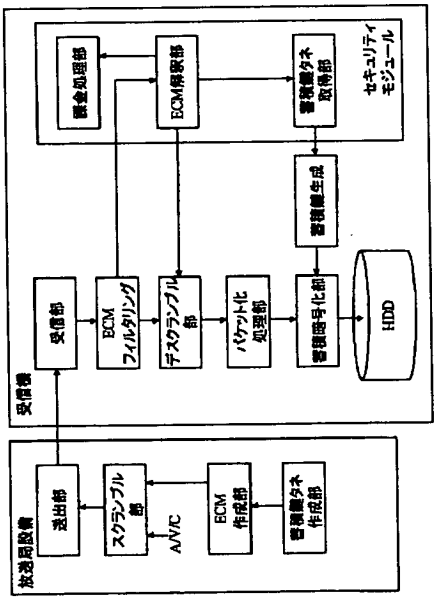
(22)出願日　平成12年７月10日(2000.7.10)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　松尾　隆史
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　井上　哲也
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

最終頁に続く

(54)【発明の名称】　番組蓄積方法及び番組蓄積装置

(57)【要約】
【課題】　放送された場組みを蓄積し、好きなときに再生して視聴する蓄積放送方式において、安全性の高いコンディショナルアクセスを実現する限定受信方式および装置を提供する。
【解決手段】　蓄積暗号化処理を実施する際に、蓄積暗号鍵を複数生成し、蓄積パケットごとに対応する蓄積暗号鍵を変化させることを特徴とする蓄積暗号化処理部を設けることにより、蓄積したコンテンツに対して高いセキュリティを確保することができる。



1

【特許請求の範囲】

【請求項１】　蓄積鍵タネを生成する蓄積鍵タネ生成部と、蓄積鍵タネを含んだECMを作成するECM作成部と、データを暗号化するスクランブル部と、ECMおよびデータを送出する送出部とを備えた放送局設備と、
放送局からのデータを受信する受信部と、受信したデータからECMを取得するECMフィルタリング部と、ECMを解釈するECM解釈部と、受信したECMを元に課金処理を行う課金処理部と、ECMから蓄積鍵タネを取得する蓄積鍵タネ取得部と、受信したスクランブルデータを復号するデスクランブル部と、復号したデータをパケット化するパケット化処理部と、パケット化されたデータを蓄積暗号化する蓄積暗号化部と、蓄積暗号化する際に利用する蓄積鍵を蓄積鍵タネより生成する蓄積鍵生成部と、蓄積暗号化されたデータなどを蓄積するHDD部とを備えた受信機とで構成されることを特徴とする番組蓄積方法。

【請求項２】　課金処理部とECM解釈部と蓄積鍵タネ取得部とをセキュリティモジュール内に持たせることを特徴とする請求項1記載の番組蓄積方法。

【請求項３】　パケット化処理部でパケット化されたデータを蓄積暗号化する蓄積暗号化部において、パケットごとに蓄積鍵を変化させることを特徴とする請求項1記載の番組蓄積方法。

【請求項４】　蓄積暗号化部で生成した蓄積付帯データと蓄積タネ取得部で取得した蓄積鍵タネとから複数の蓄積鍵を生成する蓄積鍵生成部を備えることを特徴とする請求項２記載の番組蓄積方法。

【請求項５】　蓄積暗号化部で生成した蓄積付帯データと蓄積タネ取得部で取得した蓄積鍵タネと乱数から複数の蓄積鍵を生成する蓄積鍵生成部を備えることを特徴とする請求項２記載の番組蓄積方法。

【請求項６】　蓄積鍵タネを送出部より番組情報で送付することを特徴とする請求項1記載の番組蓄積方法。

【請求項７】　蓄積鍵タネを送出部よりＰＳＩ／ＳＩで送付することを特徴とする請求項1記載の番組蓄積方法。

【請求項８】　蓄積鍵タネを蓄積暗号鍵生成部で生成することを特徴とする請求項1記載の番組蓄積方法。

【請求項９】　蓄積暗号化対象パケット毎に暗号化種別を持たせ、どの蓄積暗号鍵と対応するかを明記する暗号化種別付与部を設けることを特徴とする請求項1記載の番組蓄積方法。

【請求項１０】　暗号化種別がフラグであることを特徴とする請求項９記載の番組蓄積方法。

【請求項１１】　暗号化種別が番号であることを特徴とする請求項９記載の番組蓄積方法。

【請求項１２】　蓄積鍵タネ生成部において蓄積鍵タネを複数生成し、蓄積暗号化処理部で蓄積鍵タネを複数利用することを特徴とする請求項１記載の番組蓄積方法。

【発明の詳細な説明】

2

【０００１】

【発明の属する技術分野】ＨＤＤ付の受信機を利用し、映像音声番組や、データ放送番組などのコンテンツを蓄積し、再生時に課金するシステムにおいて、蓄積時の高いセキュリティを持つことを特徴とする番組蓄積方法に関する。

【０００２】

【従来の技術】番組を蓄積し、再生時に蓄積する技術は、特開平8-125651「信号処理装置」にも記載されている。

【０００３】この特許では、第1の暗号初期値より配信時暗号鍵を生成し、配信時暗号鍵群で配信暗号を解く。その後、第1の暗号初期値と同じく電波により配信された第2の暗号初期値より、蓄積暗号鍵を生成し、蓄積暗号化してHDDなどに蓄積する。

【０００４】

【発明が解決しようとする課題】ただし、上記技術では、以下のような課題が存在する。

１．鍵はコンテンツに対して一つのみである。このため、鍵が一つとなることで、セキュリティレベルが低下するおそれがある。リアルタイム映像配信では、数秒に一度暗号鍵を更新しているため、同程度のセキュリティを確保する必要がある。鍵が一つだけではセキュリティが低い。

２．ただし、鍵を複数にしようとすると、鍵の管理が必要となり、コンテンツの鍵切り替えタイミングとの同期を取ることが難しくなる。配信時と蓄積時の鍵の個数や暗号タイミングなどが考慮されていない。

３．番組をプレビューをしようとすると、プレビューエリアと本購入エリアとで鍵が同一となるため、受信機の制御次第で不正が容易となる。

【０００５】

【課題を解決するための手段】前記課題を解決するため、第一に、鍵のタネから蓄積暗号鍵を複数生成し、蓄積パケットごとに対応する蓄積暗号鍵を変化させることを特徴とする蓄積暗号化処理部を設けたことにある。さらに上記に加え、蓄積鍵生成に対して、乱数要素を加えることにより、同じ時刻であっても受信機ごとに鍵を異なるようにすることも可能となる。

【０００６】第二に、コンテンツには、パケットごとに時刻情報（タイムスタンプ）などの順番情報をつけ、順番情報と生成された鍵とを同期させることを特徴とする蓄積暗号化処理部を設けたことにある。さらに、コンテンツのパケットに、暗号化種別を判別するフラグを持たせることにより、鍵の切り替えを明示的にすることも可能となる。

【０００７】第三に、蓄積鍵タネを複数生成し送付し、「プレビュー用鍵」と「本購入用鍵」の２つを用意することを特徴とするECM生成部を設けたことにある。これにより、プレビュー部分にはプレビュー用鍵を利用し、

その他の部分は本購入用鍵を利用して暗号化を行うことが可能となり、プレビューを行うシステムにおいて高いセキュリティを確保することが可能となる。

【０００８】

【発明の実施の形態】本発明の実施例を以下に示す。

【０００９】放送局は、課金を行う番組ごとにECM(番組情報)を作成し、ECMに埋め込まれたスクランブル鍵で映像／音声／データコンテンツを暗号化（スクランブル）する。その後、送出部において、スクランブル化されたコンテンツとECMを多重化して送出する。

【００１０】受信機では、受信を行った後に受信されたデータよりECMだけをフィルタリングしてセキュリティモジュールに渡す。セキュリティモジュールは、ICカードやＰＣＭＣＩＡカードなどで提供されるほか、受信機内に機能的に埋め込まれることもある。

【００１１】セキュリティモジュールでは、取得したＥＣＭより、蓄積鍵タネ取得部で蓄積鍵タネを取得し、これを受信機に渡す。受信機は、ＩＣカードより蓄積鍵タネを受け取ると、蓄積鍵タネを元にして複数の蓄積鍵を生成する。蓄積鍵は、コンテンツを分割配信する際の番号情報などと蓄積鍵タネとから生成され、一つの蓄積鍵がコンテンツ中のどの部分の蓄積鍵が該当するかがわかるように生成されている。蓄積鍵を生成するために必要となる情報としては、パケットと共に埋め込まれた時刻情報や、パケットのパケット番号などが挙げられる。コンテンツは、ＥＣＭにより取得されたスクランブル鍵によりデスクランブル部においてデスクランブルされ、その後蓄積暗号化部により、蓄積鍵により暗号化され、ＨＤＤに蓄積される。また、蓄積の際には、ＥＣＭもあわせてＨＤＤ内に蓄積される。ＥＣＭの蓄積形態としては、配信されたままの状態でコンテンツパケット内に埋め込まれる場合、一つのＥＣＭだけ切り出されて蓄積される場合などがある。また、ECMを蓄積する場合には、蓄積時のセキュリティを高めるために、ECMの暗号を変換する、さらに2重に暗号をかける、ECMのフォーマットを変えるなどの処理も効果的である。また、セキュリティモジュール内の蓄積メモリ領域が確保できる場合には、ECMは、受信機内ではなく、セキュリティモジュールに蓄積することによりセキュリティを向上させることができる。

【００１２】なお、本実施例では、ＥＣＭにより蓄積鍵タネを配信し、ＥＣＭを蓄積することにより蓄積鍵タネをＨＤＤに蓄積する方式を示したが、この他に、ＥＣＭ以外の配信手段を利用して配信する場合、受信機において蓄積鍵タネを蓄積のたびに生成し、蓄積鍵タネをＨＤＤに蓄積する場合などがある。

【００１３】さらに、上記に加え、蓄積鍵タネと蓄積鍵生成のための元情報のほかに、乱数もしくは受信機ＩＤなどを加えることにより、コンテンツが同じであっても受信機や蓄積タイミングが異なる場合に暗号化バイト列を異なるようにすることも可能となる。

【００１４】また、蓄積鍵を生成する場合に、コンテンツの各パケットの蓄積時刻を付け、その時刻を元に各パケット毎に蓄積鍵を生成する方法では、パケットが非常に小さい場合には、蓄積鍵を生成する頻度が非常に高くなり、受信機に負荷がかかる可能性がある。これを避けるために、パケットのヘッダ領域に暗号鍵種別を設定し、この暗号鍵種別を利用して生成頻度を低くすることもできる。例えば、図４に示すように、暗号鍵種別にフラグを持たせ「Ｅｖｅｎ」および「Ｏｄｄ」の値をとるようにすると、フラグが切り替えられた時点の時刻を元に蓄積鍵を生成し、次にフラグが切り替わるまではその蓄積鍵を利用する、と言う仕組みを持たせることによって蓄積鍵生成間隔をあけることが可能となる。また、暗号鍵種別をフラグではなく番号にすることにより、よりわかりやすく切り替えを示すことも可能となる。

【００１５】また、コンテンツにプレビュー期間を設定する場合には、従来のスクランブル手法では、プレビュー期間にはスクランブルを解くためのスクランブル鍵をセキュリティモジュールより提供し、プレビュー可能期間以外の期間では、スクランブルを解かないようにスクランブル鍵を渡さない、という処理を行っている。本方式では、一つのコンテンツに対してプレビュー期間に対応する蓄積鍵タネと、本購入時取得可能となるコンテンツの部分の蓄積鍵タネの２つを分けることにより、プレビュー視聴の場合にはプレビュー用の蓄積鍵タネをセキュリティモジュールから受信機に渡し、本購入まで行った場合には、図５に示すとおり、プレビュー視聴用の蓄積鍵タネと本購入用鍵タネとを渡すことにより、暗号化の鍵と暗号化対象部とを明確に切り分けることが可能となり、セキュリティレベルを向上させることが可能となる。

【００１６】次に、蓄積された番組を購入し再生する場合の処理を以下に示す（図３参照）。

【００１７】視聴者が購入操作を実施すると、受信機はＨＤＤに蓄積されたＥＣＭをセキュリティモジュールに渡す。セキュリティモジュールは、受け取ったＥＣＭを元にして課金処理を実施し、課金が正常に完了した場合に蓄積鍵タネを受信機に対して渡す。受信機は、蓄積鍵タネを元にして、蓄積時と同様に複数の蓄積鍵を生成する。生成された蓄積鍵を利用して、コンテンツの蓄積暗号を解き、ＡＶデコーダにおいてコンテンツを再生／実行する。

【００１８】

【発明の効果】ＨＤＤ付受信機で、コンテンツを蓄積し、再生時に課金するシステムにおいて、蓄積時のセキュリティレベルを向上させることが可能となる。

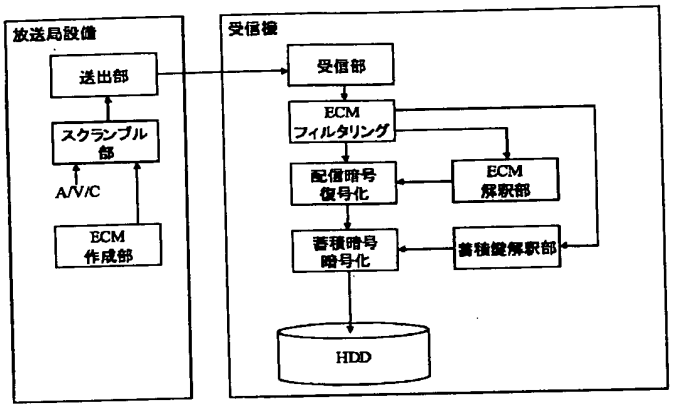
【図面の簡単な説明】

【図１】従来システムの構成例を示す図

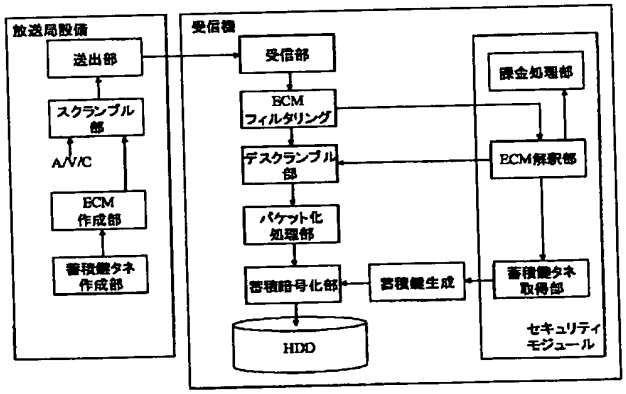
【図２】蓄積時における本発明の構成例を示す図

【図３】再生時における本発明の構成例を示す図
【図４】コンテンツの蓄積パケットの例を示す図
【図５】プレビュー用鍵の利用例を示す図

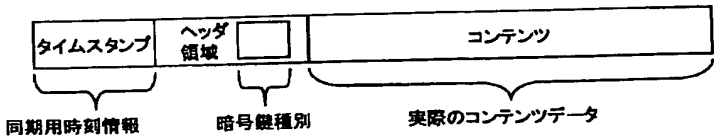
【図１】



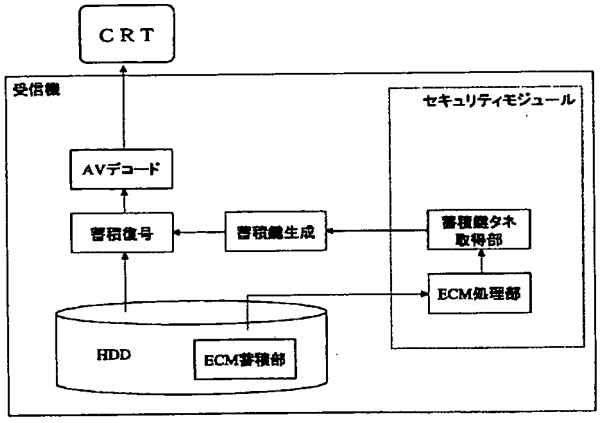
【図２】



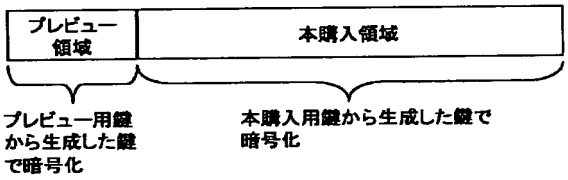
【図４】



【図３】



【図５】



フロントページの続き

(51)Int.Cl.7	識別記号	FI		テーマコード（参考）
Ｈ０４Ｎ	5/765	Ｈ０４Ｌ	9/00	６０１Ｅ
	5/781	Ｈ０４Ｎ	5/781	５１０Ｃ
	7/16		7/167	Ｚ
	7/167			

(72)発明者　村上　弘規
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　庭野　智
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　東　吾紀男
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　中原　徹
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　深見　幸靖
愛知県名古屋市中区栄２丁目６番１号白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内

Ｆターム(参考)　5C025 BA25 BA27 BA30 DA10
5C063 AB05 AC01 AC05 CA23 CA31 DA07
5C064 CA18 CB01 CC01
5J104 AA11 AA16 EA04 EA22 NA02 NA35 PA05